

DOCKET NO.: 273868US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SATO

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/19713

INTERNATIONAL FILING DATE: December 22, 2004

FOR: ENCRYPTING APPARATUS AND ENCRYPTING METHOD

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313


Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2004-048457	24 February 2004

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/19713. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

22.12.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

20 JAN 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2004年 2月24日

出 願 番 号
Application Number: 特願2004-048457
[ST. 10/C]: [JP2004-048457]

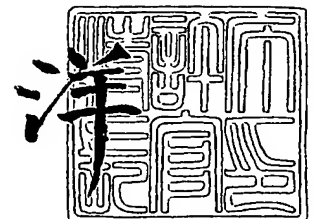
出 願 人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年12月 3日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 0390531102
【提出日】 平成16年 2月24日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 H04K 1/00
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号ソニー株式会社内
 【氏名】 佐藤 英雄
【特許出願人】
 【識別番号】 000002185
 【氏名又は名称】 ソニー株式会社
【代理人】
 【識別番号】 100082740
 【弁理士】
 【氏名又は名称】 田辺 恵基
【手数料の表示】
 【予納台帳番号】 048253
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9709125

【書類名】 特許請求の範囲**【請求項 1】**

秘匿対象の情報を暗号化する暗号化装置において、
内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、上記素子群における固有パラメータを生成する生成手段と、
上記生成手段により生成された上記固有パラメータを用いて上記情報を暗号化する暗号化手段と
を具えることを特徴とする暗号化装置。

【請求項 2】

上記生成手段は、
互いに異なる複数の評価パターンを記憶する記憶手段を具え、
上記記憶手段に記憶された各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する
ことを特徴とする請求項 1 に記載の暗号化装置。

【請求項 3】

所定の通信相手と通信する通信手段を具え、
上記生成手段は、
上記通信相手から要求された各上記評価パターンを、上記記憶手段に記憶された各上記評価パターンのなかから選択し、当該選択した各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する
ことを特徴とする請求項 2 に記載の暗号化装置。

【請求項 4】

所定の撮像対象を撮像する固体撮像素子を具え、
上記生成手段は、
均一な上記撮像対象の撮像結果として上記固体撮像素子から出力される信号に基づいて、
上記固体撮像素子における上記固有パラメータを生成する
ことを特徴とする請求項 1 に記載の暗号化装置。

【請求項 5】

所定の撮像対象を撮像する固体撮像素子を具え、
上記生成手段は、
均一な上記撮像対象の撮像結果として上記固体撮像素子から出力される信号に基づいて、
上記固体撮像素子における上記固有パラメータを生成するパラメータ生成手段と、
生体の表面又は上記生体の内方の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記生体固有の生体情報を生成する生体情報生成手段とを具え、
上記暗号化手段は、
上記パラメータ生成手段により生成された上記固有パラメータを用いて、上記生体情報生成手段により生成された上記生体情報を暗号化する
ことを特徴とする請求項 1 に記載の暗号化装置。

【請求項 6】

秘匿対象の情報を暗号化する暗号化方法において、
内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、上記素子群における固有パラメータを生成する第 1 のステップと、
生成した上記固有パラメータを用いて上記情報を暗号化する第 2 のステップと
を具えることを特徴とする暗号化方法。

【請求項 7】

上記第 1 のステップでは、
互いに異なる複数の評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する
ことを特徴とする請求項 6 に記載の暗号化方法。

【請求項 8】

上記第 1 のステップでは、

各上記評価パターンのなかから、所定の通信相手からの要求に対応する各上記評価パターンを選択し、当該選択した各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する

ことを特徴とする請求項 7 に記載の暗号化方法。

【請求項 9】

上記第 1 のステップでは、

均一な撮像対象の撮像結果として固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成する

ことを特徴とする請求項 6 に記載の暗号化方法。

【請求項 10】

上記第 1 のステップでは、

均一な撮像対象の撮像結果として固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成するパラメータ生成ステップと、

生体の表面又は上記生体の内方の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記生体固有の生体情報を生成する生体情報生成ステップと

を具え、

上記第 2 のステップでは、

上記固有パラメータを用いて上記生体情報を暗号化する

ことを特徴とする請求項 6 に記載の暗号化方法。

【書類名】明細書

【発明の名称】暗号化装置及び暗号化方法

【技術分野】

【0001】

本発明は、暗号化装置及び暗号化方法に関し、例えば識別対象の正当性を証明するための情報（以下、これを認証情報と呼ぶ）を暗号化する場合に適用して好適なものである。

【背景技術】

【0002】

従来、秘密鍵暗号方式又は公開鍵暗号方式に準拠した暗号化装置は、認証情報に対して、内部の不揮発性メモリに記憶された暗号鍵情報を用いて所定の暗号化処理を施すことにより暗号認証情報を生成し、これを復号化装置に送信するようになされている。

【0003】

この場合、暗号化装置は、不揮発性メモリに記憶された暗号鍵情報の盗用をも防止して暗号機能の信頼性を確保するようになされており、当該暗号鍵情報の盗用を防止する手法として、暗号化装置内の深層部における所定の部材間に不揮発性メモリを搭載する手法、あるいは、不揮発性メモリと、当該不揮発性メモリに暗号鍵情報を記憶しておくときだけ暗号化する暗号復号化部を1つのチップとして搭載する手法（例えば特許文献1参照）がある。

【特許文献1】特開2003-256282公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところでかかる暗号化装置においては、不揮発性メモリを搭載する際に煩雑化するのみならず、当該不揮発性メモリを搭載するものによる暗号鍵情報の盗用を避け得ず、この結果、暗号機能の信頼性を得るには未だ不十分であった。

【0005】

本発明は以上の点を考慮してなされたもので、暗号機能の信頼性を向上し得る暗号化装置及び暗号化方法を提案しようとするものである。

【課題を解決するための手段】

【0006】

かかる課題を解決するため本発明においては、秘匿対象の情報を暗号化する暗号化装置において、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、当該素子群における固有パラメータを生成する生成手段と、この生成手段により生成された固有パラメータを用いて情報を暗号化する暗号化手段とを設けるようにした。

【0007】

また本発明においては、秘匿対象の情報を暗号化する暗号化方法において、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、当該素子群における固有パラメータを生成する第1のステップと、生成した固有パラメータを用いて情報を暗号化する第2のステップとを設けるようにした。

【発明の効果】

【0008】

以上のように本発明によれば、内部に有する素子群における固有パラメータを用いて情報を暗号化するようにしたことにより、不揮発性メモリ等に予め保持させなくとも製造時であっても第三者には知り得ない固有パラメータを用いて暗号化することができるため、当該認証情報D1の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。

【発明を実施するための最良の形態】

【0009】

以下図面について本発明の一実施の形態を詳述する。

【0010】

(1) 認証システムの構成

図1において、1は全体として本実施の形態による認証システムの構成を示し、通信元の複数の暗号化装置2(2A~2N)と、その通信相手の復号化装置3とが無線により接続されることにより構成されており、当該暗号化装置2と復号化装置3とが相互に各種情報を送受信することができるようになされている。

【0011】

この場合、暗号化装置2は、復号化装置3との通信時にこの暗号化装置2を使用する使用者の所定部位における特徴パターンを認証情報として生成する。そして暗号化装置2は、この認証情報に対して所定の暗号化処理を施すことにより暗号認証情報を生成し、これを復号化装置3に送信するようになされている。

【0012】

一方、復号化装置3は、このとき受信した暗号認証情報に対して所定の復号化処理を施すことにより認証情報を復元し、この認証情報を予め登録された対応する登録情報と照合する。

【0013】

そして復号化装置3は、この照合結果に基づいて、このとき認証情報を送信した暗号化装置2を使用する使用者が正規の登録者であると判断した場合にのみ引き続き暗号化装置2との情報の授受を行うようになされている。

【0014】

このようにしてこの認証システム1は、暗号化装置2を使用する使用者の正当性を、当該使用者自身の生体情報を用いて判断するようになされている。

【0015】

(2) 暗号化装置の構成

暗号化装置2(2A~2N)は、それぞれ同一の構成であることによりここでは暗号化装置2Aの構成について説明する。

【0016】

この暗号化装置2Aは、図2に示すように、指内方の血管を撮像対象として撮像する撮像部11と、当該撮像部11の撮像結果に基づいて認証情報を生成する認証情報生成部12と、当該認証情報を暗号化する暗号化部13と、所定の無線通信方式に準拠した通信処理を実行して情報の送受信を行う通信部14とによって構成される。

【0017】

この撮像部11は、撮像部11は、血管内の脱酸素化ヘモグロビン(静脈血)又は酸素化ヘモグロビン(動脈血)に近赤外線帯域の光(近赤外光)が特異的に吸収されることを利用して、当該血管を撮像するようになされている。

【0018】

實際上、撮像部11は、図3に示すように、近赤外光を発射する1又は2以上の光源21を有し(図3では3つの光源を例として図示している)、光源21から発射される近赤外光の光路上には、当該近赤外光のうち特定の近赤外線帯域の光を透過する第1のフィルタ22、当該第1のフィルタ22を介して得られる光のうち静脈血に吸収される近赤外線帯域とその付近との光を透過する第2のフィルタ23及び固体撮像素子24が順次配置される。

【0019】

またこの撮像部11には、近赤外光の光路上以外の位置(以下、これを光路外位置と呼ぶ)P1に散光板25が設けられており、この散光板25は、光路外位置P1と、固体撮像素子24から所定距離を隔てた前面の位置(以下、これを光路上位置と呼ぶ)P2との間を移動自在となっている。

【0020】

そしてこの撮像部11においては、第1のフィルタ22と第2のフィルタ23との間に指FGを介挿することができるようになされていると共に、当該指FGの介挿時に近赤外光の光路に対する雰囲気中の外光の入射を遮蔽する遮蔽部26が設けられており、これに

より指FG内方における血管の撮像時に遮蔽部24外における可視光や紫外光による近赤外光への影響を低減することができるようになされている。

【0021】

この場合、撮像部11は、第1及び第2のフィルタ22、23間に指FGが介挿された状態において撮像命令コマンドが与えられると、光源21から近赤外光を発射し、これを第1のフィルタ22を介して指FGに照射する。

【0022】

この近赤外光は指FG内方における血管組織では内在するヘモグロビンに特異的に吸収されるため、当該指FGを経由して得られる近赤外光は血管組織の形成パターンを表す血管パターン光として、第2のフィルタ23を介して固体撮像素子24に入射することとなる。

【0023】

そして撮像部11は、かかる血管パターン光を固体撮像素子24に配された複数の光電変換素子により光電変換し、これら光電変換素子において生成された血管画像信号S1を認証情報生成部12(図2)に送出する。

【0024】

このようにして撮像部11は、生体内方に有する血管を撮像対象として撮像することができるようになされている。

【0025】

認証情報生成部12は、供給される血管画像信号S1に対してA/D(Analog/Digital)変換処理を施すことにより血管画像データを生成し、この血管画像データに基づく血管画像のうち、予め指定された領域に有する血管を抽出する。そして認証情報生成部12は、抽出した血管の形成パターンを認証情報D1として生成し、これを暗号化部13に送出する。

【0026】

暗号化部13は、所定のアルゴリズムにより順次生成された複数の暗号鍵情報を記憶するメモリ(以下、これを暗号鍵情報記憶メモリと呼ぶ)13aを有しており、当該暗号鍵情報記憶メモリ13aに記憶された複数の暗号鍵情報D2(D2₁~D2_n)のうち、通信部11を介して復号化装置3(図1)からの指定要求に対応する例えば暗号鍵情報D2₁を選択し、これを読み出す。

【0027】

そして暗号化部13は、供給される認証情報D1に対して、このとき読み出した暗号鍵情報D2₁を用いて例えばAES(Advanced Encryption Standard)に準拠した暗号化処理を施すことにより暗号認証情報D3を生成し、これを通信部14を介して復号化装置3(図1)に送信するようになされている。

【0028】

このように暗号化装置2Aは、生体内方に有する固有の血管形成パターンを認証情報D1として生成することにより、当該生体表面に有する指紋等を認証情報として生成する場合に比して生体からの直接的な盗用を防止できるため、暗号化装置2Aを使用する使用者が登録者になりすますといった事態を未然に回避することができるようになされている。

【0029】

(3) 暗号鍵情報生成処理

かかる構成に加えて、この暗号化装置2Aは、撮像部11における均一な撮像対象の撮像結果に基づいて、この暗号化装置2A固有の複数の暗号鍵情報D2(D2₁~D2_n)を生成するようになされている。

【0030】

この場合、暗号化装置2Aは、復号化装置3(図1)から通信部14を介して暗号鍵情報の生成要求を受けるごとに所定の暗号鍵情報生成処理をその都度実行し、この結果得られた暗号鍵情報D2を暗号化部13の暗号鍵情報記憶メモリ13aに記憶又は更新するようになされている。以下、この暗号鍵情報生成処理を実行する暗号鍵情報生成部15につ

いて説明する。

【0031】

この暗号鍵情報生成部15は、復号化装置3からの生成要求があった場合に、撮像部11に対して均一な撮像対象を撮像させ、当該撮像した結果得られる信号に基づいて暗号鍵情報を生成するようになされている。

【0032】

實際上、暗号鍵情報生成部15は、撮像部11（図3）の散光板25が光路外位置P1から光路上位置P2に配置されるように制御すると共に、撮像部11に撮像命令コマンドを送出する。

【0033】

この場合、撮像部11（図3）では、光源21から発射された近赤外光は、第1及び第2のフィルタ23、24を順次介して散光板25に照射され、当該散光板25において固体撮像素子24に対して均一な拡散光（以下、これを均一拡散光と呼ぶ）として拡散されて、固体撮像素子24に入射することとなる。

【0034】

ここで、この固体撮像素子24には、当該固体撮像素子24に格子状に配された複数の光電変換素子に対応させて開口部及び集光レンズがそれぞれ設けられているが、これら開口部及び集光レンズの形状には製造工程上の様々な要因によってばらつきがあり、このばらつきが固体撮像素子24固有となっている。

【0035】

従って、固体撮像素子24での均一拡散光に対する光電変換結果として暗号鍵情報生成部15（図2）に入力される信号（以下、これを均一画像信号と呼ぶ）S2には、製造時には知り得ない固体撮像素子24固有のばらつきがノイズパターン（以下、これをばらつきパターンと呼ぶ）として含まれることとなる。

【0036】

そして暗号鍵情報生成部15は、このようにして得られた均一画像信号S2に対してA/D変換処理を施すことにより均一画像データを生成し、この均一画像データに基づいて固体撮像素子24における固有のばらつきパターンに起因するパラメータ（以下、これを素子固有パラメータと呼ぶ）を生成する。

【0037】

この実施の形態の場合、暗号鍵情報生成部15では、かかる素子固有パラメータを生成する手法として、均一画像データに対する所定の評価パターンと均一画像データとのハミング距離を算出し、当該算出結果を素子固有パラメータとして生成する手法が採用されている。

【0038】

具体的に暗号鍵情報生成部15は、互いにハミング距離の離れた例えば3つのデータ列が評価パターンA_{EV}、B_{EV}、C_{EV}として記憶された情報記憶メモリ15aを有しており、これら評価パターンA_{EV}、B_{EV}、C_{EV}を用いて、均一画像データのうち評価パターンと同一データ長となる上位の均一画像データ（以下、これを上位均一画像データと呼ぶ）を「X」とし、排他的論理和（XOR）を「^」とすると、次式

【0039】

【数 1】

$$dH(x, A_{EV}) = \sum x_i \wedge A_i = X_a$$

$$dH(x, B_{EV}) = \sum x_i \wedge B_i = X_b \quad \dots\dots (1)$$

$$dH(x, C_{EV}) = \sum x_i \wedge C_i = X_c$$

但し、 $i = 1 \sim n$

【0040】

に従って、上位均一画像データXと、評価パターン A_{EV} 、 B_{EV} 、 C_{EV} それぞれとのハミング距離 X_a 、 X_b 、 X_c をそれぞれ算出し、これらハミング距離 X_a 、 X_b 、 X_c を所定の順序で組み合わせ、当該組み合わせを素子固有パラメータとして生成するようになされている。

【0041】

この場合、暗号鍵情報生成部15は、上位均一画像データXと各評価パターン A_{EV} 、 B_{EV} 、 C_{EV} との相関結果を素子固有パラメータとして生成するため、撮像時の撮像状態に応じて均一画像データが変化した場合であっても、ばらつきパターンに起因する素子固有パラメータの再現性を維持することができるようになされている。

【0042】

またこの場合、暗号鍵情報生成部15は、製造後の固体撮像素子24から出力される均一画像信号S2に基づいて素子固有パラメータを生成するため、当該固体撮像素子24の製造者に対して知り得ない情報として生成することができるのみならず、当該固体撮像素子24のばらつきパターン自体ではなく各評価パターン A_{EV} 、 B_{EV} 、 C_{EV} との相関結果の組み合わせを素子固有パラメータとして生成するため、この暗号化装置2の製造者や固体撮像素子24を盗用したものに対しても知り得ない情報として生成することができるようになされている。

【0043】

次いで暗号鍵情報生成部15は、このようにして生成した素子固有パラメータをシードとして所定のアルゴリズムにより複数の暗号鍵情報D2 ($D_{21} \sim D_{2n}$)を生成し、当該暗号鍵情報D2を暗号化部13の暗号鍵情報記憶メモリ13aに記憶又は更新するようになされている。

【0044】

この結果、暗号化部13に供給される認証情報D1は、この暗号化装置(固体撮像素子24)固有の例えば暗号鍵情報D₂₁を用いた暗号化処理により暗号認証情報D3として生成され、通信部14を介して復号化装置3に送信されることとなる。

【0045】

なお、暗号鍵情報生成部15は、新たに複数の暗号鍵情報D2を生成した場合には、所定の登録処理により又は暗号鍵情報D2に対して所定の暗号化処理を施した後に復号化装置3に送信することにより、当該新たに生成した複数の暗号鍵情報D2を復号化装置3のデータベースに登録しておくようになされている。

【0046】

このようにこの暗号化装置2は、製造時には知り得ない素子固有パラメータから導出した暗号鍵情報D2を用いて認証情報D1を暗号化することにより、暗号化装置2を使用する使用者の登録者へのなりすましをより回避して暗号機能の信頼性を格段に高めることができるようになされている。

【0047】

(4) 復号化装置の構成

復号化装置3は、図4に示すように、所定の無線通信方式に準拠した通信処理を実行して情報の送受信を行う通信部30と、暗号化装置2(2A~2N)に対して各種要求を行う要求部31と、当該通信部30で受信された結果得られる暗号認証情報D3を復号化する復号化部32と、当該復号化部32での復号結果を用いて所定の認証処理を実行する照合部33と、登録データベースDBとによって構成される。

【0048】

この登録データベースDBには、所定の登録処理により、暗号化装置2(2A~2N)の撮像部11で撮像される血管と同一部位における血管の形成パターンと、当該暗号化装置2(2A~2N)の固体撮像素子24における同一の素子固有パラメータから導出された複数の暗号鍵情報D2とがそれぞれ登録情報D10(D10₁~D10_n)として登録されている。

【0049】

この場合、要求部31は、通信部30を介して接続した暗号化装置2(2A~2N)に対して、所定のタイミングで認証処理時における各種条件を要求するようになされており、当該条件として複数の暗号鍵情報のうち、使用する暗号鍵情報D2₁、D2₂、……、又はD2_nの番号やその他の事項を要求する。この場合、要求部31は、指定した暗号鍵情報の番号を復号化部32に通知するようになされている。

【0050】

また要求部31は、必要に応じて暗号鍵情報D2の生成を要求するようになされており、この場合、登録データベースDBに登録された対応する登録情報D10₁、D10₂、……、又はD10_nの暗号鍵情報D2を、所定の登録処理又は通信部30を介して得られる暗号化装置2によって新たに生成された暗号鍵情報に更新するようになされている。

【0051】

復号化部32は、通信部30を介して供給される暗号認証情報D3のヘッダに記述される送信元アドレスに基づいて、登録データベースDBのなかから例えば暗号化装置2Aに対応する登録情報D10₁を読み出し、当該登録情報D10₁の複数の暗号鍵情報D2₁~D2_nのうちこのとき要求部31から通知された暗号化情報D2₁を選択する。

【0052】

そして復号化部32は、暗号認証情報D3に対して、このとき選択した暗号鍵情報D2₁を用いて暗号化装置2Aと同一の暗号化処理を施すことにより認証情報D1を復元し、当該認証情報D1及び対応する登録情報D10₁を照合部33に送出する。

【0053】

照合部33は、供給される認証情報D1の血管形成パターンと、対応する登録情報D10₁の血管形成パターンとを所定の手法により照合するようになされており、この照合結果として所定の合致率が得られなかった場合には、このとき認証情報D1を送信した暗号化装置2Aを使用する使用者が不正使用する第三者であると判断し、その後の暗号化装置2Aとの情報の授受を停止するように通信部30を制御する。

【0054】

これに対して照合部34は、所定の合致率が得られた場合には、このとき認証情報D1を送信した暗号化装置2Aを使用する使用者が正規の使用者であると判断し、この場合には暗号化装置2Aと、内部に設けられた情報処理部(図示せず)との間で情報の授受を行うように通信部31を制御するようになされている。

【0055】

このようにして復号化装置3は、生体固有の認証情報D1(血管形成パターン)と、固体撮像素子24固有の固有素子パラメータから導出された暗号鍵情報D2とを用いて認証処理を実行することができるようになされている。

【0056】

(5) 本実施の形態による動作及び効果

以上の構成において、この暗号化装置2(2A~2N)は、撮像部11における均一な撮像対象の撮像結果として固体撮像素子24から出力される均一画像信号S2に基づいて

、当該固体撮像素子 24 固有の素子固有パラメータを生成する。

【0057】

そして暗号化装置 2 (2A~2N) は、この素子固有パラメータから導出した所定の暗号鍵情報 D2 を用いて認証情報 D1 を暗号化する。

【0058】

従って暗号化装置 2 (2A~2N) は、従来のように不揮発性メモリ等に予め暗号化鍵を保持させなくとも、製造時であっても第三者には知り得ない素子固有パラメータから導出した暗号鍵情報 D2 を生成することができるため、当該認証情報 D1 の秘匿性を簡易に確保することができる。

【0059】

以上の構成によれば、均一な撮像対象の撮像結果として固体撮像素子 24 から出力される均一画像信号 S2 に基づいて当該固体撮像素子 24 固有の素子固有パラメータを生成し、この素子固有パラメータから導出した所定の暗号鍵情報 D2 を用いて認証情報 D1 を暗号化するようにしたことにより、認証情報 D1 の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。

【0060】

(6) 他の実施の形態

なお上述の実施の形態においては、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、素子群における固有パラメータを生成する生成手段として、固体撮像素子 24 に配された複数の光電変換素子から出力される均一画像信号 S2 に基づいて、当該固体撮像素子 24 における固有の素子固有パラメータを生成するようにした場合について述べたが、本発明はこれに限らず、例えばタッチパッドの圧電素子群から出力される信号に基づいて固有パラメータを生成するようにしても良く、この他種々の能動素子や受動素子の集合を単位とする素子群における固有パラメータを生成することができる。

【0061】

この場合、素子群は、単一種類であっても複数種類であっても上述の実施の形態と同様の効果を得ることができる。

【0062】

また固有パラメータの生成手法として、素子群から出力される均一画像信号 S2 のデータを、直接、記憶手段としての情報記憶メモリに記憶された互いに異なる 3 つの評価パターン A_{EV}、B_{EV}、C_{EV} との間におけるハミング距離 (相関値) を算出し、これら算出結果を所定順序で組み合わせるようにした場合について述べたが、本発明はこれに限らず、均一画像信号 S2 のデータに対して FFT (Fast Fourier Transform) 処理を施し、この処理結果と評価パターン A_{EV}、B_{EV}、C_{EV} とのハミング距離の算出結果を組み合わせるようにしても良く、あるいは FFT 処理結果のうち低周波成分のデータのみに対して逆 FFT 処理を施し、この処理結果と評価パターン A_{EV}、B_{EV}、C_{EV} とのハミング距離の算出結果を組み合わせるようにしても良く、又はこれら処理結果を組み合わせるようにしても良い。このようにすれば、より秘匿性の高くかつ再現性の優れた固有パラメータを生成することができるため、暗号機能の信頼性を格段に向上することができる。

【0063】

この場合、撮像部 11 に対して散光板 25 を撮像させ、当該撮像結果として得られる信号に基づいて固有パラメータを暗号鍵情報として生成する暗号鍵情報生成部 15 を適用するようにしたが、本発明はこれに限らず、散光板 25 以外の均一な撮像対象を撮像させるようにしても良く、また暗号鍵情報を生成せずに固有パラメータのみを生成するようにしても良く、要は、固有パラメータを生成するこの他種々の生成部を適用することができる。

【0064】

またこの場合、生成時期として、復号化装置 3 から通信部 14 を介して暗号鍵情報の生成要求を受けるごとに生成するようにした場合について述べたが、本発明はこれに限らず、製造時にのみ生成する等、この他種々のタイミングで生成することができる。

【0065】

さらに評価パターンとして、所定の評価パターンを予め情報記憶メモリに記憶するようにしたが、本発明はこれに限らず、複数の評価パターンを情報記憶メモリに記憶しておく、この評価パターンのうちから予め規定された数の評価パターンを選択するようにしても良く、またこのとき選択する評価パターンを復号化装置3の要求に応じて変更するようにしても良く、あるいは所定タイミング時に所定のアルゴリズムにより生成した評価パターンを情報記憶メモリに記憶するようにしても良い。このようにすれば、仮に、認証情報D1が盗用された場合及び暗号鍵情報から評価パターンが解読された場合であっても、対応する評価パターンを用いないようにすることができるため、暗号機能の信頼性を格段に向上することができる。

【0066】

さらに評価パターンの数として、3種類の評価パターンを情報記憶メモリに記憶するようにしたが、本発明はこれに限らず、少なくとも2以上の評価パターンを情報記憶メモリに記憶していれば、上述の実施の形態と同様の効果を得ることができる。

【0067】

また上述の実施の形態においては、固有パラメータを用いて情報を暗号化する暗号化手段として、固有パラメータから導出した暗号鍵情報を用いて血管形成パターンからなる認証情報D1を暗号化する暗号化部13を適用するようにした場合について述べたが、本発明はこれに限らず、固有パラメータにより認証情報D1を暗号化する暗号化部を適用するようにしても良い。

【0068】

この場合、生体内方の血管形成パターンを認証情報D1として暗号化するようにしたが、本発明はこれに限らず、例えば指紋等の生体表面の特徴パターン等、この他種々の生体情報を認証情報として暗号化することができ、また認証情報や生体情報である必要はなく、要は、秘匿対象とすべき情報を暗号化すれば良い。

【産業上の利用可能性】

【0069】

本発明は、パーソナルコンピュータや携帯電話機等の端末装置や、家庭用電子機器等の装置であって、外部の装置に対して自身を識別させる場合に利用可能である。

【図面の簡単な説明】

【0070】

【図1】 認証システムの構成を示すブロック図である。

【図2】 本実施の形態による暗号化装置の構成を示すブロック図である。

【図3】 撮像部の構成を示す略線図である。

【図4】 復号化装置の構成を示すブロック図である。

【符号の説明】

【0071】

1……認証システム、2……暗号化装置、3……復号化装置、11……撮像部、12……認証情報生成部、13……暗号化部、13a……暗号鍵情報メモリ、15……暗号鍵情報生成部、15a……情報記憶メモリ、24……固体撮像素子。

【書類名】 図面
【図 1】

1

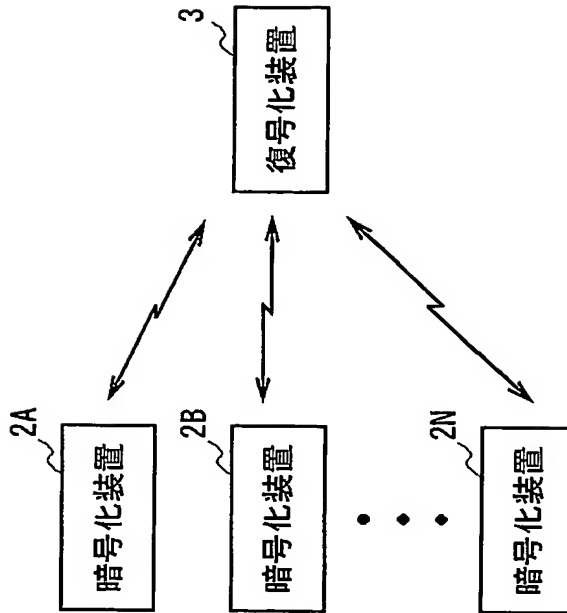


図 1 認証システムの構成

【図 2】

2A(2B~2N)

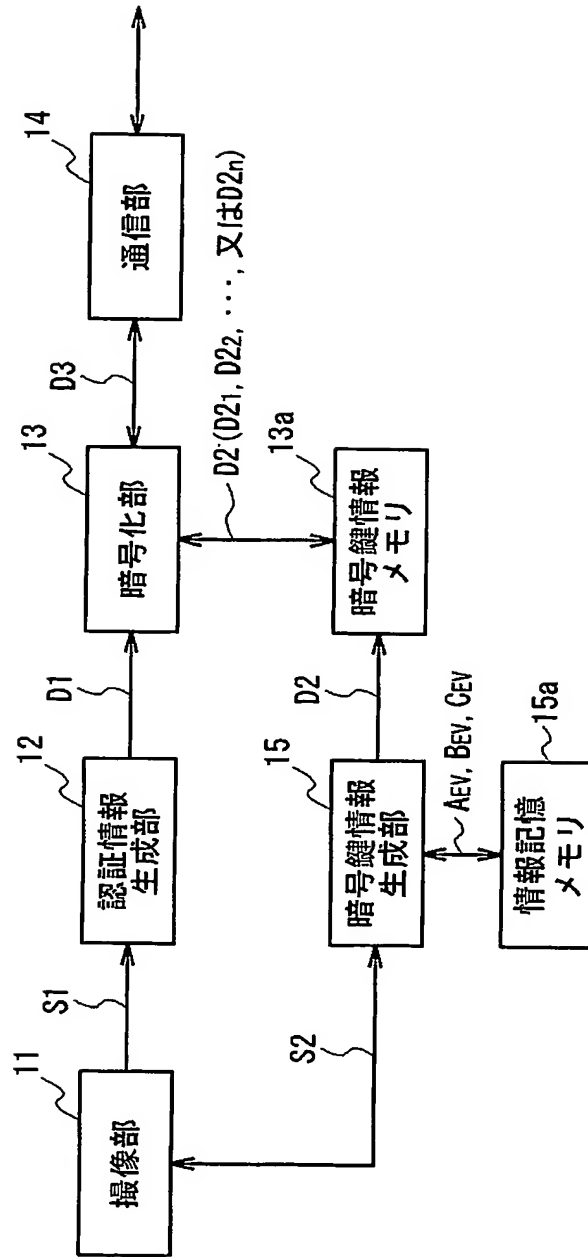


図 2 暗号化装置の構成

【図 3】

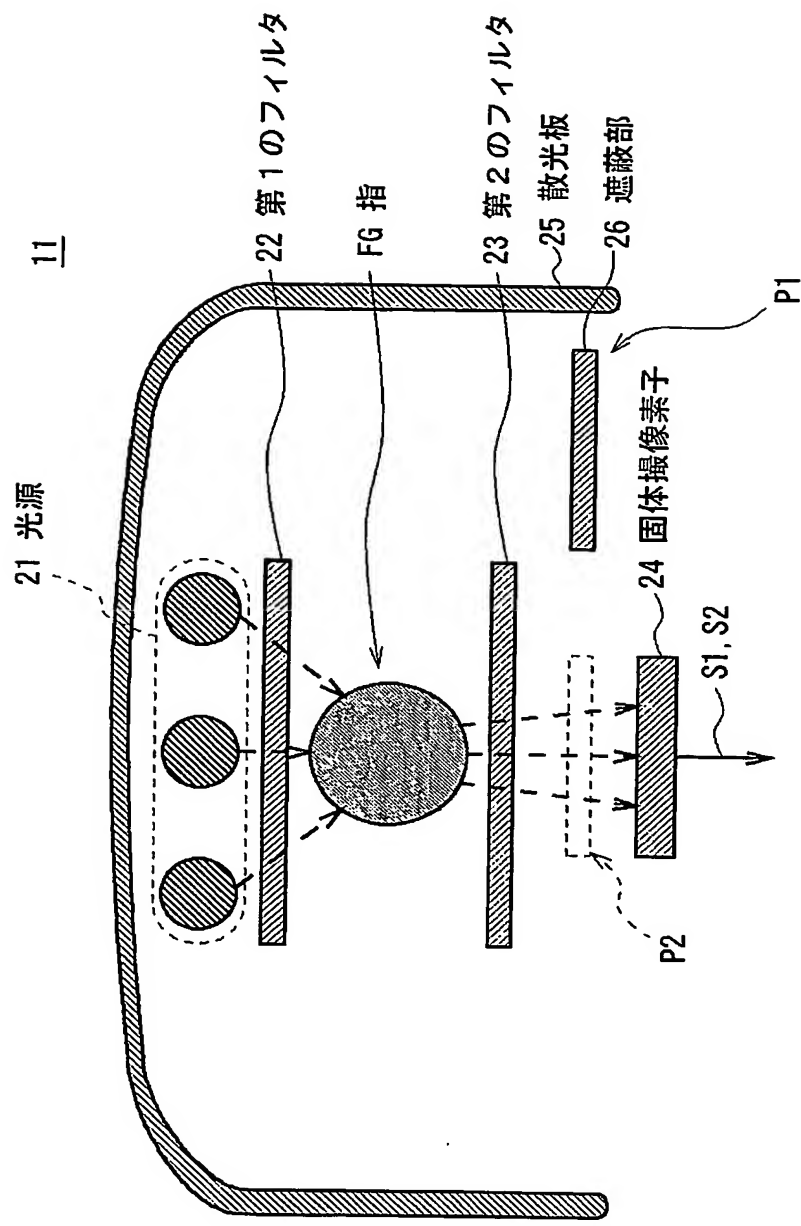


図 3 撮像部の構成

【図 4】

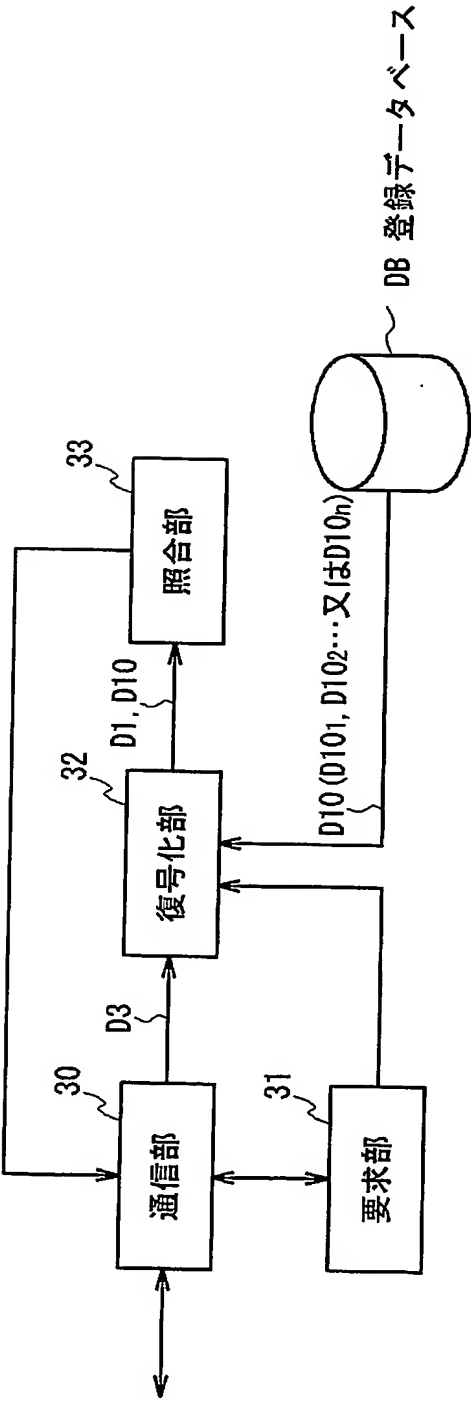


図 4 復号化装置の構成

【書類名】 要約書

【要約】

【課題】

暗号機能の信頼性を向上し得る暗号化装置及び暗号化方法を提案する。

【解決手段】

撮像部 11 における均一な撮像対象の撮像結果として固体撮像素子から出力される均一画像信号 S2 に基づいて当該固体撮像素子固有の素子固有パラメータを生成し、この素子固有パラメータから導出した暗号鍵情報 D2 を用いて認証情報 D1 を暗号化するようにしたことにより、認証情報 D1 の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。

【選択図】 図 2

特願 2004-048457

ページ: 1/E

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社